FUTURA

Google Play Store : ces applis à supprimer le plus vite possible !

Podcast écrit et lu par Adèle Ndjaki

[Générique d'intro, une musique énergique et vitaminée.]

Quand de simples applis mobiles peuvent devenir votre pire cauchemar, c'est le décryptage de la semaine dans *Vitamine Tech*.

[Fin du générique.]

Possesseurs de smartphones Android, faites attention à vous, la menace rôde ! Google vous met en garde, plusieurs applications sont à supprimer au plus vite de vos appareils ! Mais pourquoi ? Bonjour à toutes et à tous, je suis Adèle Ndjaki et aujourd'hui dans *Vitamine Tech*, on parle du danger que représentent diverses applis mobiles.

[Une musique électronique calme.]

Vous avez peut-être, sans le savoir, des applications dangereuses sur votre téléphone. Et pourtant... elles viennent du Google Play Store ! Google tire la sonnette d'alarme, suite à une découverte inquiétante faite par les experts en cybersécurité du Cyble Research and Intelligence Labs, ou CRIL. Ils ont repéré plus d'une vingtaine d'applications malveillantes qui sont passées entre les mailles du filet et se sont retrouvées disponibles au téléchargement comme si de rien n'était. Leur apparence ? Tout ce qu'il y a de plus normal. Certaines sont même bien notées. Elles prétendent vous aider à gérer vos portefeuilles de cryptomonnaies. Mais en réalité... ce sont des arnaques très bien conçus. Le piège est simple : vous installez une application qui semble sérieuse, vous l'ouvrez, et là... sans le savoir, vous tombez sur un faux site déguisé, un phishing masqué en appli mobile. Pendant que vous l'utilisez, l'application collecte vos informations personnelles, et dans certains cas, elle peut même accéder à vos identifiants bancaires ou à ceux de vos comptes en cryptomonnaie. Ce qui rend ces applications encore plus dangereuses, c'est qu'elles imitent des applis très connues du monde des cryptos. À première vue, il est presque impossible de faire la différence. Moralité de l'histoire : même une appli qui semble fiable peut cacher une attaque bien pensée.

[Virgule sonore, une cassette que l'on accélère puis rembobine.]

[Une musique de hip-hop expérimental calme.]

Ce n'est pas la première fois que le Play Store de Google se retrouve au cœur d'une affaire de sécurité majeure. L'an dernier, une opération baptisée Konfety a révélé un vaste réseau

d'applications malveillantes sur Android : plus de 250 applis infectées, des millions de téléchargements. Leur technique ? Les "evil twins" ou "jumeaux maléfiques", un système d'évasion ultra sophistiqué pour contourner les détecteurs. Résultat : vols de données, fraudes pub, installation de malwares... Un vrai cauchemar numérique. Et aujourd'hui, rebelote. Avec l'aide des chercheurs du Cyble Research Lab, Google a identifié une nouvelle vague d'applis à risque. Et certaines sont encore actives sur des milliers de téléphones, à l'insu des utilisateurs. Voici les premières à supprimer : Pancake Swap, Suiet Wallet, Hyperliquid, Raydium, BullX Crypto, OpenOcean Exchange, Meteora Exchange, SushiSwap et Harvest Finance Blog. Si l'une d'elles est sur votre smartphone, agissez au plus vite ! Après avoir supprimé les applications suspectes de votre téléphone, la première chose à faire, c'est de sécuriser vos comptes. Récupérez l'accès à vos portefeuilles numériques en passant uniquement par les sites ou applications officielles, changez vos mots de passe, et si vous remarquez la moindre activité étrange, n'attendez pas : signalez immédiatement le problème et transférez vos fonds vers une plateforme reconnue et sécurisée. Autre geste important : Google insiste aussi sur le fait d'activer la protection intégrée de votre smartphone Android. Il s'agit de Play Protect, un outil de sécurité proposé par Google qui vérifie en continu les applications installées sur votre appareil. Pour l'activer, c'est simple : ouvrez le Play Store, appuyez sur votre photo de profil, puis cherchez la section Play Protect. Là, vous pourrez voir si le scan automatique est activé. Sinon, il suffit d'un clic pour le mettre en marche. Ce type de vérification ne prend que quelques secondes, mais peut vraiment faire la différence pour éviter les mauvaises surprises.

[Virgule sonore, un grésillement électronique.]

C'est tout pour cet épisode de *Vitamine Tech*. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le dernier épisode de Futura Santé dans lequel Melissa Lepoureau vous parle en profondeur de la maladie de Lyme ! Pour le reste, je vous remercie pour votre fidélité à Vitamine Tech, je vous souhaite tout le meilleur, et, comme d'habitude, une excellente journée ou une très bonne soirée et rester branché !

[Un glitch électronique ferme l'épisode.]